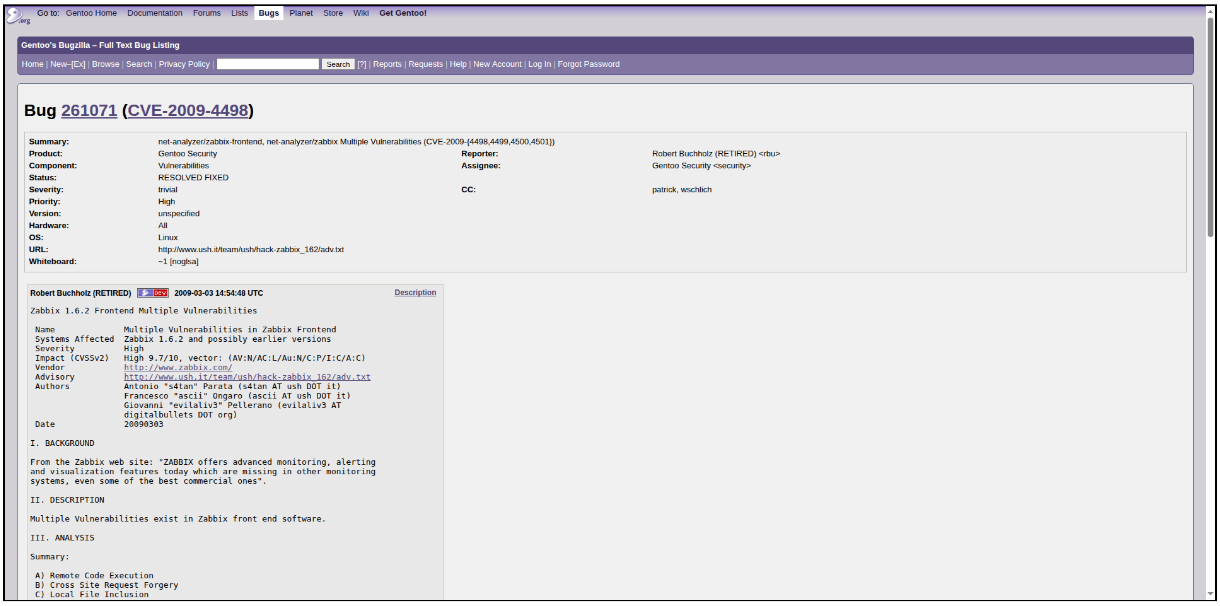
# PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

| | |
|---|---|
| **Source URL:** | https://bugs.gentoo.org/show_bug.cgi?format=multiple&id=261071 |
| **Archived Date:** | August 15, 2025 at 15:10 |
| **Document Type:** | Web Page Archive |
| **Wayback Machine:** | https://web.archive.org/web/*/https://bugs.gentoo.org/show_bug.cgi?format=multiple&id=261071 |

## Page Screenshot


Go to: Gentoo Home Documentation Forums Lists Bugs Planet Store Wiki Get Gentoo!
Gentoo's Bugzilla – Full Text Bug Listing
Home | New–[Ex] | Browse | Search | Privacy Policy | Search [?] | Reports | Requests | Help | New Account | Log In | Forgot Password

**Bug 261071 (CVE-2009-4498)**

| | | | |
|---|---|---|---|
| **Summary:** | net-analyzer/zabbix-frontend, net-analyzer/zabbix Multiple Vulnerabilities (CVE-2009-{4498,4499,4500,4501}) | | |
| **Product:** | Gentoo Security | **Reporter:** | Robert Buchholz (RETIRED) <rbu> |
| **Component:** | Vulnerabilities | **Assignee:** | Gentoo Security <security> |
| **Status:** | RESOLVED FIXED | | |
| **Severity:** | trivial | **CC:** | patrick, wschlich |
| **Priority:** | High | | |
| **Version:** | unspecified | | |
| **Hardware:** | All | | |
| **OS:** | Linux | | |
| **URL:** | http://www.ush.it/team/ush/hack-zabbix_162/adv.txt | | |
| **Whiteboard:** | ~1 [noglsa] | | |

**Robert Buchholz (RETIRED)** Dev **2009-03-03 14:54:48 UTC** Description

```
Zabbix 1.6.2 Frontend Multiple Vulnerabilities

 Name              Multiple Vulnerabilities in Zabbix Frontend
 Systems Affected  Zabbix 1.6.2 and possibly earlier versions
 Severity          High
 Impact (CVSSv2)   High 9.7/10, vector: (AV:N/AC:L/Au:N/C:P/I:C/A:C)
 Vendor            http://www.zabbix.com/
 Advisory          http://www.ush.it/team/ush/hack-zabbix_162/adv.txt
 Authors           Antonio "s4tan" Parata (s4tan AT ush DOT it)
                   Francesco "ascii" Ongaro (ascii AT ush DOT it)
                   Giovanni "evilaliv3" Pellerano (evilaliv3 AT
                   digitalbullets DOT org)
 Date              20090303

I. BACKGROUND

From the Zabbix web site: "ZABBIX offers advanced monitoring, alerting
and visualization features today which are missing in other monitoring
systems, even some of the best commercial ones".

II. DESCRIPTION

Multiple Vulnerabilities exist in Zabbix front end software.

III. ANALYSIS

Summary:

 A) Remote Code Execution
 B) Cross Site Request Forgery
 C) Local File Inclusion
```

# Bug 261071 (CVE-2009-4498)

| | | | |
|---|---|---|---|
| **Summary:** | net-analyzer/zabbix-frontend, net-analyzer/zabbix Multiple Vulnerabilities (CVE-2009-{4498,4499,4500,4501}) | | |
| **Product:** | Gentoo Security | **Reporter:** | Robert Buchholz (RETIRED) <rbu> |
| **Component:** | Vulnerabilities | **Assignee:** | Gentoo Security <security> |
| **Status:** | RESOLVED FIXED | | |
| **Severity:** | trivial | **CC:** | patrick, wschlich |
| **Priority:** | High | | |
| **Version:** | unspecified | | |
| **Hardware:** | All | | |
| **OS:** | Linux | | |
| **URL:** | http://www.ush.it/team/ush/hack-zabbix_162/adv.txt | | |
| **Whiteboard:** | ~1 [noglsa] | | |

**Robert Buchholz (RETIRED)** Dev **2009-03-03 14:54:48 UTC** Description

```
Zabbix 1.6.2 Frontend Multiple Vulnerabilities

 Name              Multiple Vulnerabilities in Zabbix Frontend
 Systems Affected  Zabbix 1.6.2 and possibly earlier versions
 Severity          High
 Impact (CVSSv2)   High 9.7/10, vector: (AV:N/AC:L/Au:N/C:P/I:C/A:C)
 Vendor            http://www.zabbix.com/
 Advisory          http://www.ush.it/team/ush/hack-zabbix_162/adv.txt
 Authors           Antonio "s4tan" Parata (s4tan AT ush DOT it)
                   Francesco "ascii" Ongaro (ascii AT ush DOT it)
                   Giovanni "evilaliv3" Pellerano (evilaliv3 AT
                   digitalbullets DOT org)
 Date              20090303

I. BACKGROUND

From the Zabbix web site: "ZABBIX offers advanced monitoring, alerting
and visualization features today which are missing in other monitoring
systems, even some of the best commercial ones".

II. DESCRIPTION

Multiple Vulnerabilities exist in Zabbix front end software.

III. ANALYSIS

Summary:

 A) Remote Code Execution
 B) Cross Site Request Forgery
 C) Local File Inclusion

...

patches seem to be here [svn://svn.zabbix.com/branches/1.6]:

------------------------------------------------------------------------
r6625 | artem | 2009-01-21 15:17:42 +0100 (Wed, 21 Jan 2009) | 1 line

 - [DEV-282] fixes frontend vulnerabilities (Artem)
------------------------------------------------------------------------
r6623 | artem | 2009-01-21 15:08:41 +0100 (Wed, 21 Jan 2009) | 1 line

 - [DEV-282] fixes frontend vulnerabilities (Artem)
------------------------------------------------------------------------
r6621 | artem | 2009-01-21 13:58:05 +0100 (Wed, 21 Jan 2009) | 1 line

 - [DEV-282] fixes frontend vulnerabilities (Artem)
```

**Christian Hoffmann (RETIRED)** Dev **2009-04-14 18:09:47 UTC** Comment 1

```
Although we only ship this in ~arch, can we put some focus on this bug? It allows
for remote code execution.
```

**Christian Hoffmann (RETIRED)** Dev **2009-05-18 18:23:35 UTC** Comment 2

```
Adding net-analyze/zabbix[frontend] which ships the same code.. no idea why we have
both split package and an "allround" package.
Maybe we should consider masking this for now, as noone seems to actively maintain
it currently? I'm using it myself, but I don't know if/when I'll have time to work
on it.
```

**Stefan Behte (RETIRED)** Dev Sec **2010-01-08 20:41:28 UTC** Comment 3

```
CVE-2009-4498 (http://nvd.nist.gov/nvd.cfm?cvename=CVE-2009-4498):
  The node_process_command function in Zabbix Server before 1.8 allows
  remote attackers to execute arbitrary commands via a crafted request.

CVE-2009-4499 (http://nvd.nist.gov/nvd.cfm?cvename=CVE-2009-4499):
  SQL injection vulnerability in the get_history_lastid function in the
  nodewatcher component in Zabbix Server before 1.6.8 allows remote
  attackers to execute arbitrary SQL commands via a crafted request,
  possibly related to the send_history_last_id function in
  zabbix_server/trapper/nodehistory.c.

CVE-2009-4500 (http://nvd.nist.gov/nvd.cfm?cvename=CVE-2009-4500):
  The process_trap function in trapper/trapper.c in Zabbix Server
  before 1.6.6 allows remote attackers to cause a denial of service
  (crash) via a crafted request with data that lacks an expected :
  (colon) separator, which triggers a NULL pointer dereference.

CVE-2009-4501 (http://nvd.nist.gov/nvd.cfm?cvename=CVE-2009-4501):
  The zbx_get_next_field function in libs/zbxcommon/str.c in Zabbix
  Server before 1.6.8 allows remote attackers to cause a denial of
  service (crash) via a request that lacks expected separators, which
  triggers a NULL pointer dereference, as demonstrated using the
  Command keyword.

CVE-2009-4502 (http://nvd.nist.gov/nvd.cfm?cvename=CVE-2009-4502):
  The NET_TCP_LISTEN function in net.c in Zabbix Agent before 1.6.7,
  when running on FreeBSD or Solaris, allows remote attackers to bypass
  the EnableRemoteCommands setting and execute arbitrary commands via
  shell metacharacters in the argument to net.tcp.listen.  NOTE: this
  attack is limited to attacks from trusted IP addresses.
```

**Patrick Lauer** Dev **2010-01-09 13:04:07 UTC** Comment 4

```
# Patrick Lauer <patrick@gentoo.org> (09 Jan 2010)
# Package has been unsplit, use net-analyzer/zabbix
net-analyzer/zabbix-agent
net-analyzer/zabbix-frontend
net-analyzer/zabbix-server

+  09 Jan 2010; Patrick Lauer <patrick@gentoo.org> -zabbix-1.4.6.ebuild,
+  -zabbix-1.6.5.ebuild, -zabbix-1.6.5-r1.ebuild, -zabbix-1.6.6.ebuild,
+  -zabbix-1.6.6-r1.ebuild:
+  Remove old

That should bring all ebuilds to useful versions.
```

**Stefan Behte (RETIRED)** Dev Sec **2010-01-09 14:13:10 UTC** Comment 5

```
Thanks!
BTW: CVE-2009-4502 does not apply to us, removing.

Closing noglsa.
```